



Strong forces combine to create a significant challenge



The competence requirements of IT security people are constantly rising



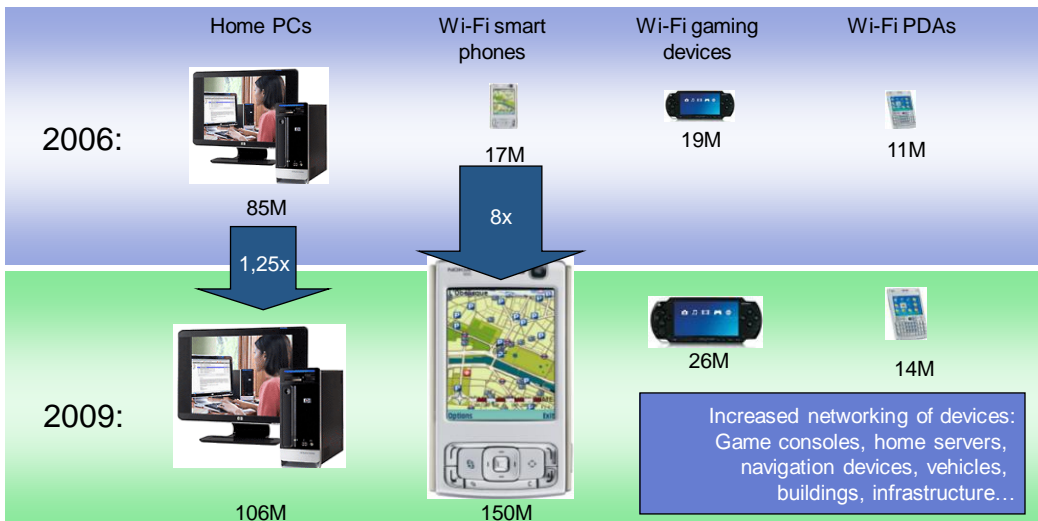
New technologies and changes in user behaviour increases vulnerability:

- Increased use of “always-on” broadband access and wireless hotspots
- Increased use of networked applications (e.g. instant messaging, VoIP)
- Increased sharing of files (e.g. music, video, software)
- Increased workforce mobility (20-25% of all PCs are laptops)
- Increased use of multiple connected devices (e.g. PDAs, mobile phones)



15 September, 2008 Page 3

Devices access the services that connect us to our networked lives.



Source: Gartner, IDC, SA, Nokia

15 September, 2008 Page 4

Connected



a "pc-like" usage of smart phones will drive the demand for services



Connected to friends and communities on the Web

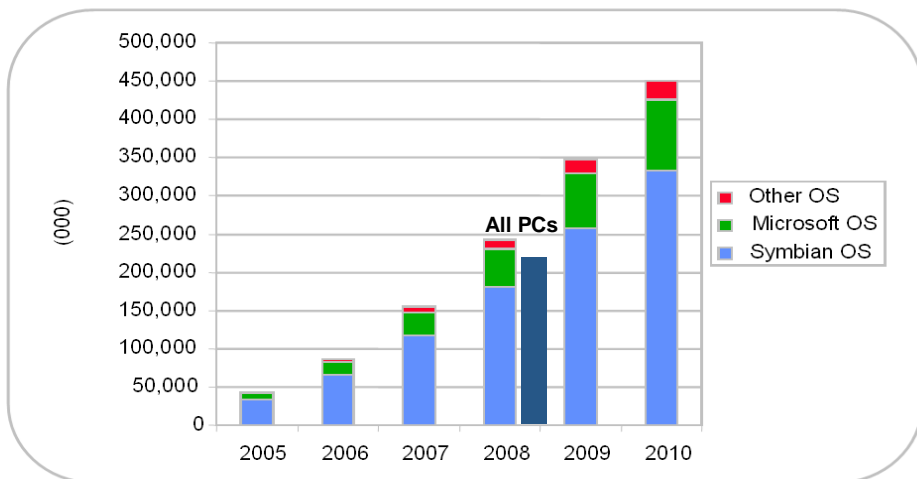


Connected to personal and business content



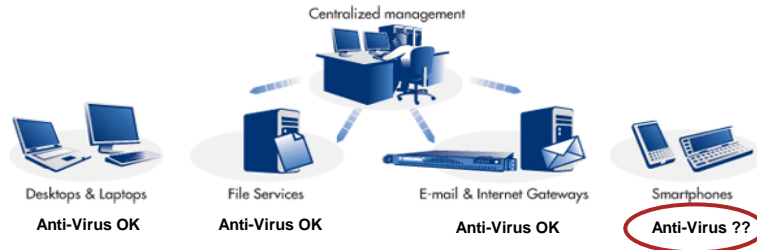
Connected via a fleet of digital devices

Projected smartphone shipments by OS



Source: Ovum, May 2006

”Smart phones are part of your IT network”



- Any unprotected device connected to both the Internet and your company LAN is a security risk.
- Security policies in many companies require protection on all devices

15 September, 2008 Page 7



Mobile Malicious Content Landscape

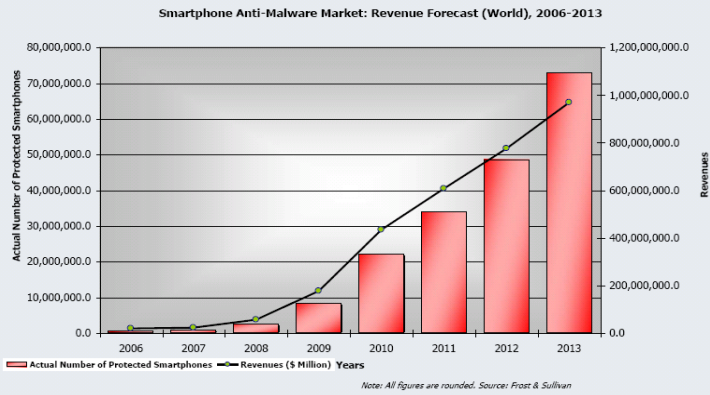


- Any open operating system enables developing malicious content
- Virus writers typically try to attack the most popular platforms
- Both virus writers and security vendors have learned from the PC world
- Antivirus is a service with a software component
- Any antivirus solution is only as good as the latest update
 - Response time is critical
 - Distribution methods are critical
- Users are not interested in security, they want to trust, not to be trusted

Latest market study from Frost&Sullivan



Market Forecasts: Aftermarket Anti-Malware Products



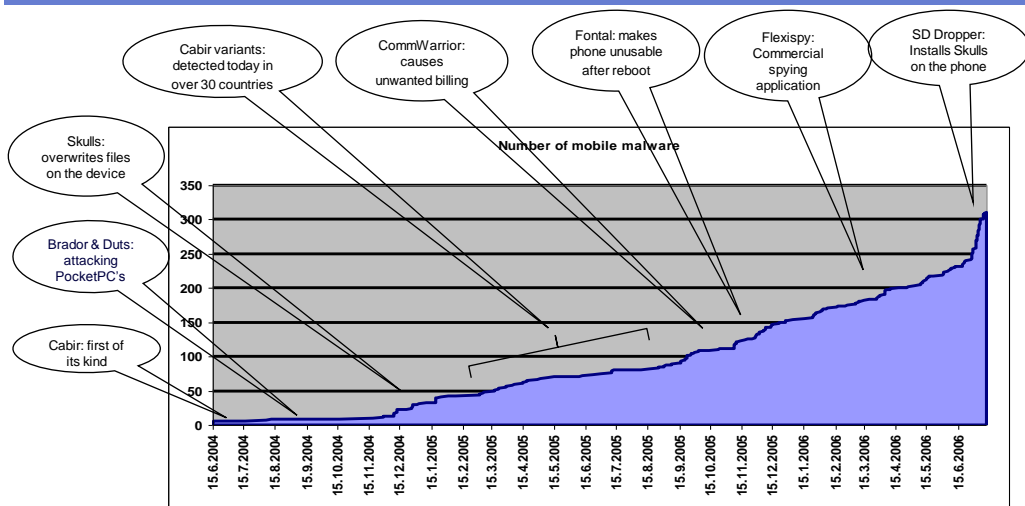
Short History of Mobile Antivirus Business



- Early days (2000 – 2003)
 - Initial hype → bubble burst → interest dropped
 - NTT DoCoMo realized threat and took action
- Hibernation (2003 – 2005)
 - Operators neglecting the issue, few antivirus companies trying to convince operators to prepare for the worst.
- Re-Activation (2005 →)
 - Operators are waking up; too little too late...?
 - All major antivirus companies are starting to push the solutions, feature game starting
 - Public is mostly unaware of any problems
- Business as usual (2007 →)
 - Mobile antivirus is seen as standard issue in smartphones. Mobile antivirus can be purchased by both individuals and corporations just like PC protection today

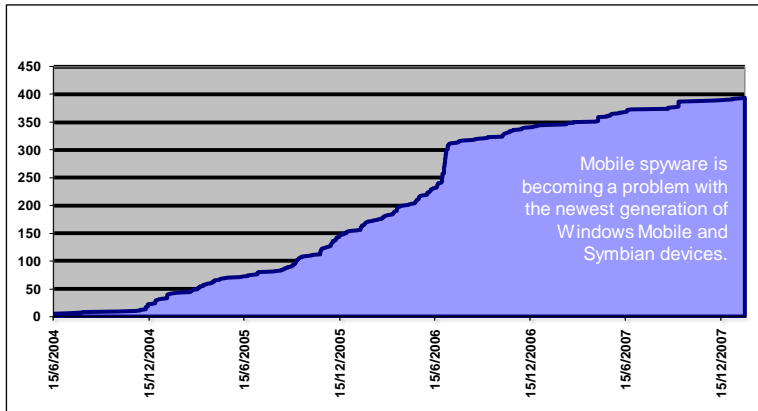
15 September, 2008 Page 11

Cumulative number of malicious content



15 September, 2008 Page 12

The mobile virus situation in Q1 2008: just reached 400



15 September, 2008 Page 13

Types Of Mobile Threats



What we have seen so far

- Viruses
- Worms
- Trojans
- Single target spying applications and spyware

What we have not seen yet

- Rootkits
- Worm that does not need user interaction for spreading
- Mass distributed spyware
- Large scale profit oriented malware

15 September, 2008 Page 14

Virus Terminology



VIRUS is a computer program that replicates by attaching itself

WORM is a computer program that replicates independently by sending itself to other systems

TROJAN HORSE is a program with hidden destructive functionality

MALWARE is a common name for all kinds of unwanted software such as viruses, worms, trojans and jokes

15 September, 2008 Page 15

Examples...

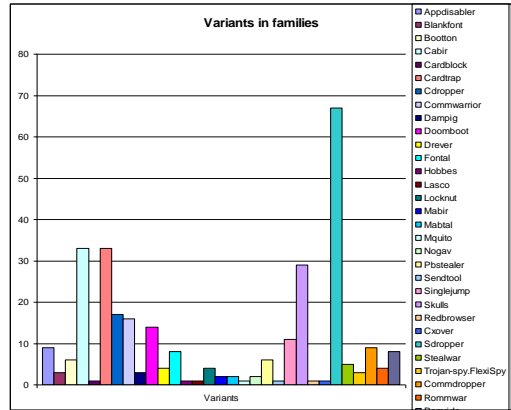
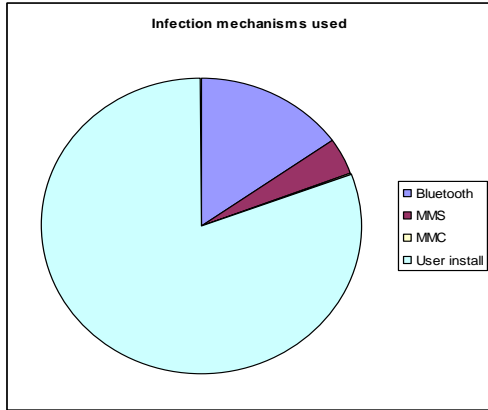


- SymbOS/Kiazha Mar 2008
- WM/InfoJack Feb 2008
- SymbOS/Hatihati.A Jan 2008
- SymbOS/Beselo Jan 2008
- An operator with 10m subscribers in Europe: 5000 Commwarrior infected devices in June 2006, in spite of gateway level filtering solution.
- An operator with more than 20m subscribers: In May 2006 there were 1500 terminals infected with Commwarrior, 8000 messages are filtered every day in the gateway level.
- Another operator: 2100 infected terminals noted in May 2006.
- An operator from central Europe with 1,5 m subscribers: 2,8% of the total subscriber base carry Commwarrior. 48% of S60 1st E edition devices are infected.
- An European operator with 14 m subscribers: Since Oct 2005 over 8000 infected. The terminals have sent 450000 MMS messages until June 2006. Largest number of messages sent by one terminal is 3500.

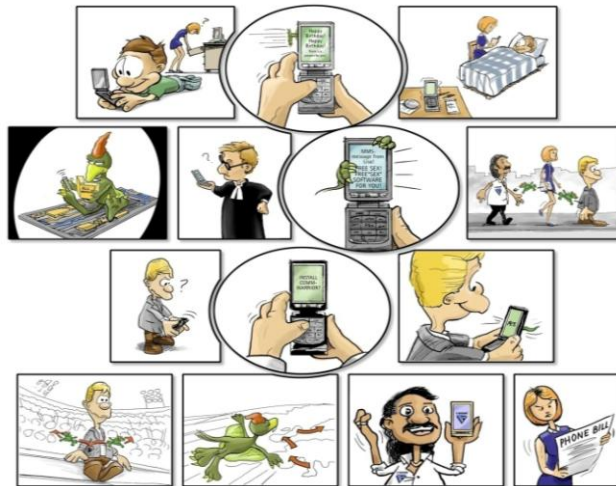


15 September, 2008 Page 16

Infection mechanisms and variant families



This could happen to you



CASE STUDY : SPYWARE



Mobile Spying Tools



Mobile spying tools are applications that are installed into a smart phone and send information out from the phone

- Typical example would be an application that sends all received SMS message to a third party without permission from the user

Mobile spying tools are not illegal by itself

- Their vendors claim that they must be used only for legal purposes
- While in reality most of the things that people use these tools are illegal. At least in countries that have strong privacy protection laws

Who Would Use Spying Tools



Some people who use PC based spying tools

- Oppressive spouses and other domestic abuse cases
- Managers spying on employees
- Industrial spies

Some vendors sell both PC and mobile spy tools

- And give discounts if you buy both
- Spy both your wife's PC and mobile phone

15 September, 2008 Page 21

Information that can be stolen by spyware



SMS and MMS traffic information and content

- Sender and receiver phone numbers and phone book names
- The content of the SMS or MMS message

E-Mail traffic information and content

- Sender and receiver addresses
- Email text and attachments

SIM card information

- Sends the SIM IMSI and phone number as soon as new SIM is inserted



15 September, 2008 Page 22

Information that can be stolen by spyware



Call information

- Incoming or outgoing call and to what number
- Time and duration of the call

Voice recording

- Application can record all phone calls to memory card
- Either the attacker needs to access the card to get recordings, or they are sent over Bluetooth, MMS or HTTP

Call interception

- Allows to tap in voice conversations by setting covert conference call

15 September, 2008 Page 23

Information that can be stolen by spyware



Remote listening

- When specific number calls the phone will answer silently
- The phone will not give any indication that call is open
- Some spyware will even allow automatic conference calls

Physical location

- Some tools are capable of using build in GPS in modern phones, and send GPS coordinates
- Those that don't use GPS send GSM cell ID and signal info

User key presses

- All user key presses can be logged and sent over SMS

15 September, 2008 Page 24

Flexispy



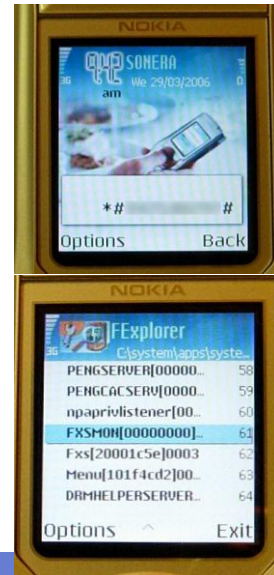
Flexispy.A was invasive enough to be classified as trojan
 Later variants are classified as spyware

Flexispy monitors

- Voice call destinations
- Voice call times dates and duration
- SMS messaging and contents

Software itself is not illegal

- Unauthorized installation of it is



Flexispy web interface



All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
ALL EVENTS 1 - 10 of 413 records									
Row Per Page 10									
Type	Direction	Duration	Contact Name	Mobile Time	Server Time				
SMS			15400	30/01/08 09:54:07	29/01/08 08:55:01				
SMS			15400	30/01/08 09:54:03	29/01/08 08:55:00				
SMS			+358407175873	08/01/08 15:22:52	07/01/08 14:23:49				
VOICE		0:00:07	0407175873	08/01/08 15:22:09	07/01/08 14:23:16				
VOICE		0:00:13	0407175873	08/01/08 14:52:38	07/01/08 13:53:50				
VOICE		0:00:00	0405081712	08/01/08 14:51:59	07/01/08 13:53:22				
E-MAIL			"Fred Savage" <fred...	07/01/08 13:25:57	07/01/08 14:26:57				
SMS			+358400648180	04/01/08 10:42:09	03/01/08 09:43:05				
VOICE		0:00:06	0400648180	04/01/08 10:41:08	03/01/08 09:42:13				
VOICE		0:00:14	0405862908	04/01/08 09:15:36	03/01/08 08:16:49				
<a>Delete <a>Refresh <a>Report Setting									
First Previous 1 2 3 4 5 Next Last									

SMS Messages



All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
Log Detail									
IMEI: 353659013790262									
Client Time: 16/01/08 13:25:05									
Server Time: 16/01/08 12:25:20									
Event Type: SMS									
Direction: OUT									
Phone Number: +358407175873									
Contact Name: Boss									
Contents: Hello.7Was the meeting about merger with Acemco tomorrow or friday. ?									
back									

15 September, 2008 Page 27

Voice Call Information



All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
Log Detail									
IMEI: 353659013790262									
Client Time: 16/01/08 13:56:03									
Server Time: 16/01/08 12:56:55									
Event Type: VOICE									
Direction: IN									
Duration: 0:00:03									
Phone Number: 0407175873									
Contact Name: Boss									
back									

15 September, 2008 Page 28

GPS Location Information



All	Voice	SMS	Email	Location	System	Search	Download	My Profile	I Need Help
Log Detail									
IMEI: 3536									
Client Time: 15/01/08 12:15:44									
Server Time: 15/01/08 11:15:58									
Event Type: LOC									
Location: Latitude: 60.163257659186									
Longitude: 24.912460640555									
72									
Cell ID:									
Cell Name:									
Network Info:									
back									

15 September, 2008 Page 29

Flexispy On Symbian S60 3rd edition



The latest versions work also on S60 3rd edition phones

- Nokia E60, E61, E65, E70, E95, N73, N95 and all other new models
- The software is **Symbian Signed**, so it passes all security checks

Flexispy has extensive capabilities including power management

- Which means that Flexispy has rights to kill other processes, such as AV applications
- Flexispy has feature that prevents “conflicting” applications, and when this feature is enabled (as per default) an Anti-Virus Solution cannot be used in that phone



15 September, 2008 Page 30



WHAT'S NEXT....



Prerequisites for a Large Malware Outbreak



Enough functionality

- for the malware to work

Enough connectivity

- for the malware to spread

Enough target terminals

- for the platform to become an interesting target



Currently 4 Types of Harmful Content



- Spreading, but not malicious
- Malicious, but not spreading
- Unwanted billing, but not malicious
- Spyware

What's next?



15 September, 2008 Page 33

It Is Already Happening...



- Reports about Cabir and Commwarrior from over 30 countries
- 13000 phones disinfected by one phone reseller chain in Greece
- The record of a single infected user was 3500 messages sent by CommWarrior
- Some operators have a viruspenetration of a few percent of all S60 devices
- Many phone service points receive infected phones almost daily
- Operators have given money back to customers infected with Commwarrior
- Operators have blocked all MMS traffic during cleaning operations
- An antivirus service point was needed during the athletics world championships in Helsinki

15 September, 2008 Page 34

Operator risks and opportunities



By neglecting the threat of mobile malware the operator risks:

- Public image as a trusted partner
- High support costs in case of widespread epidemic
- Smartphone adoption rate

By preparing, the operator:

- Has a chance to educate the media and the public in a controlled manner
- Maintains the trustworthy public image
- Has good answers for the media at a time of the epidemic
- Minimizes support costs at a time of a epidemic
- Minimizes telephone downtime
- Helps the telecom industry to maintain the unique premium status

15 September, 2008 Page 35

What Are the Minimum Requirements to Protect the Business?



1. The operating system and mobile device vendors will have to develop a security focused hot fix process for the operating systems.
2. Mobile operators must establish a gateway level security solution in the network to be able to flexibly filter the traffic
3. A real-time up-to-date antivirus client is required in all smartphones, with a mechanism for automatically delivering updates directly to the device



15 September, 2008 Page 36

What Are the Minimum Requirements to Protect the Business?



1. Corporate Security Policies have to be reviewed to include all end point devices
2. Managed solution for the mobile devices
3. In House Management or Outsourced
 - Security As A Service
4. Zero Day Protection
 - Immediate block untrusted code



15 September, 2008 Page 37

Mobile Security protects the smartphone against...



Fact: Most mobile viruses propagate using Bluetooth making a pure gateway approach insufficient in protecting subscribers against malware. The increased number of WiFi/WLAN enabled phones puts pressure on client based protection with firewall capability.



15 September, 2008 Page 38

Device Management Solution



Managed solution : easy to deploy and maintain mobile devices



15 September, 2008 Page 39

Real-time protection



15 September, 2008 Page 40

What might be coming in the future



The large number of spy tool vendors indicates that there is money in creating mobile software that is in grey area

- Most likely we will soon see mass distributed mobile spyware
- Also phishing, data stealing trojans, backdoors and other criminals tools that are used in Windows will migrate to phones

Experience has shown that where is money there will be crime

- We fear that we are going to see same development as in PC
- In PC first we had hobbyists and people with too much curiosity
- Now more than 95% of malware is created for commercial gain
- Same development will follow in mobile field

15 September, 2008 Page 41



**BE
SURE.**

